UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

KARYN NICHOLLS, SOUMENDU DAS, ROSE HARRIS, Individually and on behalf of her minor child L.I., and KELLY FREEMAN, *Plaintiffs*, v. CHANGE HEALTHCARE INC., OPTUM INC. and UNITEDHEALTH GROUP INCORPORATED., *Defendants*.	No. **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Karyn Nicholls, Soumendu Das, Rose Harris and her minor child L.I., and Kelly Freeman ("Plaintiffs"), on behalf of themselves and all others similarly situated alleges the following complaint against Defendants Change Healthcare Inc., Optum Inc., and UnitedHealth Group Incorporated (collectively "Defendants") upon personal knowledge as to their own acts, and based upon their investigation, their counsel's investigation, and information and belief as to all other matters.

INTRODUCTION

1. Defendant UnitedHealth Group ("UnitedHealth") is the largest healthcare conglomerate in the United States and its subsidiaries include both Defendant Change Healthcare, Inc. ("Change Healthcare") and Defendant Optum, Inc. ("Optum").

2. In February 2024, Defendant Change Healthcare's systems were breached by a cyberattack of unprecedented magnitude (the "data breach").[1] The data breach wreaked havoc across the US healthcare system. At least hundreds of hospitals and thousands of pharmacies have

[1] https://www.cnbc.com/2024/03/18/unitedhealth-group-paid-more-than-2-billion-to-providers-after-attack.html

been impacted. As of March 18, 2024, UnitedHealth reported it had advanced more than 2 billion dollars to providers who were impacted by the breach.[2]

3. The data breach was purportedly conducted by hackers known as "ALPHV/Blackcat", a prominent cybercriminal group known for targeting healthcare institutions. According to reports UnitedHealth paid approximately 22 million dollars in a bid to recover access to the data and systems encrypted by the "Blackcat" gang.[3]

4. According to reports, Blackcat claims to have exfiltrated more than 6 terabytes of highly sensitive data including but not limited to personal health information ("PHI"), including medical records, dental records, payment information, and claims information; personally identifiable information ("PII") including phone numbers, addresses, social security numbers, and email addresses; source code files for Change Health, and insurance records, among significant other exfiltrated information.

5. As of March 22, 2024, Defendants have yet to disclose what specific data was compromised in the attack or whether it paid Blackcat a ransom, although it is clear that, at minimum, millions of sensitive records, including medical insurance and health data, were breached.

6. The Biden Administration has also announced it is investigating the data breach due to the unprecedented magnitude of the attack.[4]

7. Defendants understand the extremely the high value of this information, including medical information, to outside parties including criminal organizations.

---

[2] https://www.unitedhealthgroup.com/newsroom/2024/2024-03-18-uhg-cyberattack-status-update.html (Last Accessed March 21, 2024)
[3] https://www.reuters.com/technology/cybersecurity/hacker-forum-post-claims-unitedhealth-paid-22-mln-ransom-bid-recover-data-2024-03-05/ (Last Accessed March 21, 2024)
[4] https://www.cnbc.com/2024/03/13/biden-administration-investigating-change-healthcare-cyberattack-as-disruptions-continue.html?&qsearchterm=ashley%20capoot (Last Accessed March 21, 2024)

8. Defendants were also aware of the increased risk of exactly this sort of data breach when UnitedHealth purchased Change Healthcare in 2021. Specifically, Defendants were warned of a risk in consolidating this sensitive medical information together.

9. Despite all the warnings Defendants received about the risk to the data they stored, including PII and PHI, Defendants did not implement adequate security measures.

10. The failure to implement adequate data security measures in the face of the obvious threat profile made a data breach entirely foreseeable, and indeed probable. But for Defendants' failure to secure and encrypt their production servers and appropriately isolate and compartmentalize data on their patients, this breach would not have occurred.

11. Members of the plaintiff class were immediately harmed because they could not purchase necessary prescription medications or had to pay exorbitant fees to do so. Plaintiffs also suffered harm in the loss of their private medical and personal information and the extreme risk of sale of this data to criminals over the dark web. Under these circumstances, Defendants unreasonably delayed in notifying individual victims of the specific information that was breached. As of March 25, 2024, Defendants have still not identified precisely what information was breached in the attack. This delay in notification to victims of the breach is unacceptable and directly harms victims of the breach, including Plaintiffs, by creating uncertainty about the extent to which they have been harmed and the need to engage in various services and efforts in the wake of the data breach, including but not limited to examining whether their PII or PHI has been sold on the dark web, taking measures to protect against identity theft crimes, expenses, and/or time spent on credit monitoring and identity theft insurance, time spent examining bank statements, time spent initiating fraud alerts, and other consequential harms.

12. Plaintiffs, individually and on behalf of all others similarly situated, allege claims of Negligence, Breach of Implied Contract, and Unjust Enrichment. Plaintiffs, individually and on behalf of all others similarly situated, ask the Court to compel Defendants to adopt reasonable information security practices to secure the sensitive PII and PHI that Defendants collect and store in their databases and to grant such other relief as the Court deems just and proper.

PARTIES

Plaintiffs

13. Plaintiff Karyn Nicholls is a resident and citizen of New Jersey who used Defendants' services. On information and belief, Ms. Nicholls's PII and PHI were compromised due to the data breach. Moreover, the breach disabled the system Ms. Nicholls uses at her pharmacy to obtain a discount on her prescribed course of the medication Zepbound. This increased the price of the medication by approximately $750. Because of this massive price spike effectively caused by the data breach, Ms. Nicholls missed her scheduled dosing and cannot continue the medication schedule. Additionally, in early March 2024, Ms. Nicholls was targeted by scammers who pretended to be from her bank and had her bank information. On information and belief, these criminals likely obtained the banking information due to Defendants' data breach.

14. Plaintiff Kelly Freeman is a resident and citizen of Indiana who used Defendants' services. On information and belief, Ms. Freeman's PII and PHI were compromised due to the data breach.

15. Plaintiff Rose Harris is a resident and citizen of Utah who used Defendants' services. On information and belief, Ms. Harris's PII and PHI were compromised due to the data breach.

16. "L.I." is a minor child of Jeff Harris and Rose Harris. On information and belief, "L.I."'s PII and PHI were compromised due to the data breach. L.I. is also a resident and citizen of Utah.

17. Plaintiff Soumendu Das is a resident and citizen of Minnesota who used Defendants' services. On information and belief, Mr. Das's PII and PHI were compromised due to the data breach.

Defendants

18. Defendant UnitedHealth Group Incorporated is the largest healthcare conglomerate in the United States. It provides care for approximately 152 million people.[5] Its annual reported revenues are in the hundreds of billions of dollars. Optum and Change Healthcare are both subsidiaries of UnitedHealth Group. It is headquartered in Minnesota and incorporated in Delaware.

19. Defendant Change Healthcare Inc. is the largest health care payment processor in the United States. It processes about 50% of all medical claims in the United States for around 900,000 physicians, 33,000 pharmacies, 5,500 hospitals, and 600 laboratories.[6] UnitedHealth completed its purchase of Change Healthcare in 2022. It is headquartered in Tennessee and incorporated in Delaware.

20. Defendant Optum Inc. is a healthcare services provider with business interests encompassing technology and related services, pharmacy care services, and various direct healthcare benefits. It has been a subsidiary of UnitedHealth since 2011. After Change Healthcare was purchased by UnitedHealth, Change Healthcare became a part of Optum.[7] Optum is headquartered in Minnesota and incorporated in Delaware.

JURISDICTION AND VENUE

21. This Court has subject matter jurisdiction and diversity jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The class contains more than 100 members (indeed, it likely contains millions or even tens of millions of members), and many of these members have citizenship diverse from Defendants. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the case in controversy.

[5] https://www.cnbc.com/2024/03/18/unitedhealth-group-paid-more-than-2-billion-to-providers-after-attack.html (Last Accessed March 21, 2024)
[6] https://www.reuters.com/technology/cybersecurity/hhs-opens-probe-into-hack-unitedhealth-unit-2024-03-13/ (Last Accessed March 21, 2024)
[7] https://www.changehealthcare.com/optum

22. The exercise of personal jurisdiction over Defendants is appropriate. Change Healthcare has its principal place of business is in Nashville, Tennessee, and all Defendants regularly conduct business in the District.

23. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because a substantial part of the events giving rise to the claims emanated from activities within this District. Specifically Change Healthcare's principal place of business is in Tennessee and Change Healthcare's breached systems, representations, decision making, and security practices are at the heart of the claims.

FACTUAL ALLEGATIONS

I. Background:

24. Defendant UnitedHealth Group is the largest healthcare insurer in the United States and processes approximately 15 billion transactions per year. Defendants Change Healthcare and Optum are wholly-owned subsidiaries of UnitedHealth. Change Healthcare combined with Optum.

25. Plaintiffs and members of the Plaintiff Class are former or current patients and consumers who used Defendants' services.

26. In order to receive treatment, Plaintiffs and members of the Plaintiff class were required to provide all or part of the following non-exclusive list of sensitive PHI and PII during the regular course of business:

- Full name and mailing or personal address,
- State and/or Federal Identification,
- Social Security Number,
- Health insurance information including but not limited to carrier, policy number, and healthcare card,
- Date of birth,
- Medical information including but not limited to information about diagnosis and treatment, personal medical history, family medical history, mental health

information, information related to STDs and treatment, medication information, and medical record number,

- Information about physicians and related medical professionals who had been involved in previous or ongoing treatment of the patient,
- Residence and travel history,
- Billing and claims information including but not limited to information related to credit and debit card numbers, bank account statements and account numbers, and insurance payment details.
- Medicare/Medicaid information.
- Information on prescriptions taken including history of taking certain prescriptions.
- Diagnostic results and treatment information.
- Information on family members including but not limited to emergency contact information and next of kin.
- Personal email addresses and phone numbers.
- Workers' comp and employment related information

27. The above information is extremely sensitive personal identifying information and personal health information (PII and PHI). This information is extremely valuable to criminals because it can be used to commit serious identity theft and medical identity theft crimes.

28. Moreover, Change Healthcare collects and aggregates significant additional information when it builds personally identifiable and assignable profiles for its clients. Thus, any information patients directly provide to Change Healthcare is only the tip of the iceberg when it comes to the overall profile of sensitive information which may have been exposed.

29. Change Healthcare for example, identifies that in addition to the information provided by patients, it also collects:

- Commercial information associated with transactions including information measuring the effectiveness of targeted information, advertisements, and offers;

- Analysis of "actual or likely preferences through a series of computer processes and add our observations to your internal profile" including for the purposes of marketing including with targeted information, advertisements and offers.
- Browser and device data including operating system and version, IP address, geographic location, browser type, device manufacturer and model, language, etc., as well as any entered search terms. They also gather device "usage" information.
- Information sent through messages or responses when using the support portal or chatbox or any other messaging services.
- Information from social media platforms including account ID and username.[8]
- Information from "other sources such as data brokers, customers, credit reporting agencies, social networks, [and] partners with which we offer co-branded services or engage in joint marketing activities [in addition to] data which may be found in the public domain.
- Publicly available records
- Government records,
- Visual information such as profile pictures.
- "Sensory Information"[9][10]

30. This additional compilation of data is extremely troubling. Not only was personal medical information and personally identifiable information that customers provided revealed to criminal hackers as a result of the data breach, but a vast quantity of additional analytical information and data may have also been exposed. Indeed, Change Healthcare expressly represents that "[t]hese other sources help us update, expand, and analyze our records; identify new customers; determine you or your organization's advertising or purchasing preferences; or

[8] The privacy policy also notes that "in some cases, the social media company may recognize you through its digital cookies even when you do not interact with their application." It references to the social media information they collect.
[9] https://www.changehealthcare.com/privacy-notice/california (Last Accessed March 21, 2024)
[10] https://www.changehealthcare.com/privacy-notice (Last Accessed March 21, 2024)

prevent or detect fraud. We combine such information with information we have collected about you through our Sites and Services."

31. Given the uses to which Change Healthcare uses this data, it is easy to imagine that criminal hackers might use it to "update, expand, and analyze their stollen PHI and PPI records;" "identify new victims;" "Determine [you] or your organization's advertising or purchasing preferences to more effectively deceive and defraud them;" and "conduct or prevent detection of fraud."

32. The aggregate PII and PHI information from millions of customers is extremely sensitive and is ideal for committing all manner of identity theft and other crimes. This combination of PII and PHI with significant other information—including information purchased from data brokers and social media websites, information on purchasing preferences, employment, and effective advertisements, and government records—is extremely personal and extremely valuable.

33. As a condition of doing business and obtaining Defendants' services and healthcare treatment, class members entrusted Defendants with this information with the explicit and implicit understanding that the information would be kept secure and that reasonable measures would be taken to maintain and ensure their security, including notification in the event of a breach, commensurate with the value of the data.

II. The Breach

34. At least as early as February 21, 2024, Change Healthcare became aware of a massive data breach of its systems.

35. The data breach impacted tens of millions of individuals across the country, although at this time it is unknown exactly how many patients had their data compromised and the extent of the data that was breached. However, given the quantity of data seized and the immense impact to Defendants' systems continuing to this day, the amount of data breached is likely immense.

36. As a result of the data breach, Change Healthcare shut down large parts of its network. More than one month after the breach, major parts of the network are still not fully functional. The large number of compromised systems indicates that Defendants did not appropriately isolate and secure them, as they should have been, given the quantity of the data they stored and the critical nature of their security for the safety and health of patients.

37. As of March 21, 2024, Defendants' website indicates the following systems are still compromised/disabled:[11]

- **Change Healthcare Enterprise (Impacts all of Change Healthcare)**

Clinical Decision Support:

- InterQual® Cloud Solutions
- InterQual® Customize
- InterQual® Review Manager – Hosted
- InterQual® Government Services

Clinical Network:

- Clinical Document Collector API
- Clinical Exchange
- Clinical Exchange Channel Partners including ePrescribe and Orders & Results
- Clinical Exchange Labs and Hospitals
- Connectivity Gateway

Cost Transparency:

- Predictive Engagement
- Provider Directory
- True View

Customer Portals:

- Client Access System
- ConnectCenter
- Customer Care Hub
- Customer Connection
- Download Central
- Download Connect
- Enrollment Central
- Vision

Dental Network:

[11] https://solution-status.optum.com (Last Accessed March 21, 2024)

- Credentialing Advocate Solution
- Dental Claim Attachments
- Dental Connect
- Dental Credentialing Manager
- Dental EDI Network
- Dental Practice Analytic Insights
- Dental Revenue Cycle Insights
- SimpleAttach Solution

Eligibility & Enrollment:

- Dual Enrollment Advocate & Recert Complete
- My Advocate
- Part D Complete & Community Advocate
- SSI Enrollment Advocate

Medical Network:

- Advanced Claim Management
- Batch Claims
- Claiming & Remittance
- Claims Automation
- Eligibility & Patient Access
- ERA Transactions
- Medical Claim Attachments
- Paper-to-EDI
- Payer Connectivity Services
- Payer Data Services
- Payer Finder website and API
- Real-time Eligibility Transactions
- Revenue Analytics

Medical Record Retrieval & Clinical Review:

- Clinical Abstraction
- Medical Record Retrieval
- Risk Adjustment Coding

Member Engagement & Experience

- Interoperability API Connector
- Member Payments
- Smart Connect, Smart Appointment Scheduling, & Clinical Care Visits

Patient Engagement & Experience

- Shop Book and Pay
- Virtual Front Desk

Payer Communications and Payment Services

- Communications Complete - Payer
- Payer Communications and Print
- Payer Enrollment Services
- Payment Network Advocate
- Settlement Advocate

Payment Integrity:

- DRG Validation
- Hospital Bill Audit
- Hospital Billing Validation/Short Stay Bill Validation

Pharmacy Benefits & TPA:

- Medicaid Pharmacy Benefits Services
- Smart Commercial Pharmacy Services

Pharmacy Solutions:

- MedRx
- Revenue Cycle Management
- SelectRx
- UPBS Analytics website
- UPBS Claims Manager website
- UPBS Claims Processing
- UPBS Configuration Manager website
- Vaccination Record

Provider Communications and Payment Services:

- Communications Complete - Provider
- Member Correspondence Advocate
- Patient Billing & Statements
- Payment Automation
- SmartPay for Providers
- SmartPay Payment Integration

Provider Network Optimization:

- Contract Manager
- Provider Manager
- Reimbursement Manager

Revenue Cycle Management:

- AccuPost
- Acuity Revenue Cycle Analytics
- Ahi Lobby
- AhiQA
- Ambulatory Claims Manager
- Assurance Reimbursement Management
- Claims & Denials Advisor

- Claims & Denials Management
- Clearance Patient Access Suite
- Financial Clearance
- National Payments Connector
- Patient Engagement Suite
- Reporting & Metrics
- Revenue Integrity
- Revenue Performance Advisor

Risk Adjustment & Quality:

- Compliance Reporter
- Dx Gap Advisor
- Edge Complete
- EMR Risk Advisor
- Encounter Complete
- Risk View

Value Based Care:

- Compliance Reporter
- Dx Gap Advisor
- Edge Complete
- EMR Risk Advisor
- Encounter Complete
- Risk View

Medical Network APIs:

- Claims Responses and Reports API
- Claims Status API
- Eligibility API
- Institutional Claims API
- Payer Finder API
- Professional Claims API

38. No healthcare provider, let alone a conglomerate as massive and well-resourced as Defendants, should ever have so many systems go down simultaneously, let alone *still have these systems down more than a month after the initial data breach*. It is common practice for sensitive servers and systems to be compartmentalized so that even if an individual system is breached, the breach will not compromise the entire enterprise and damage will be mitigated. The vast number of compromised systems suggests the existence of a fundamental security flaw

and near total failure to compartmentalize information and appropriately restrict access to only those with a "need to know" as promised by Defendants' privacy notice.

39. The breach has impacted unknown thousands of healthcare providers and pharmacies across the country and, among other things, disrupted their ability to be paid for services, as well as the ability for customers and patients, like Plaintiffs, to receive services including necessary medication and treatments.

40. As of March 25, 2024, Defendants have still not sent data breach notification letters identifying the scope and type of PII and PHI that was compromised, nor which individual patients have been harmed.

41. As of the time of filing (March 25, 2024), it is still unclear precisely how the breach occurred and exactly what measures Defendants are taking to ensure the security of their customer data and to protect against any additional breaches.

42. The scope of the Data Breach is evident and massive. It is one of the largest data breaches in the history of the United States.

III. Defendants' Privacy Representations

43. Defendants acknowledge its legal and contractual obligations to protect its clients' sensitive PII and PHI. According to Change Healthcare's online Privacy Notice, "Privacy Matters to Change Healthcare, so we follow a privacy framework that helps us to manage and protect your personal information."[12]

44. As discussed in detail above, Defendants collected vast quantities of information on their patients including aggregated information significantly beyond the already substantial PII and PHI provided directly by patients.

45. Defendants promised this information would only be accessible to those who needed it. However, given the scale of the breached systems and stolen data, Defendants clearly failed in this duty. No one person should ever have a "need" to access all the compromised systems and information under any circumstances and the massive security and network problems

[12] https://www.changehealthcare.com/privacy-notice (Last Accessed March 21, 2024)

could have been contained if Defendants had employed reasonable security practices. Defendants' unreasonable practices directly harmed Plaintiffs and class members.

IV. Defendants Failed to Comply with Reasonable Cybersecurity Standards

46. At all times relevant to this Complaint, Defendants knew or should have known the significance and necessity of safeguarding its customers' PII and PHI, and the foreseeable consequences of a data breach. Defendants knew or should have known that because it collected and maintained the PII and PHI for a significant number of customers, a significant number of customers would be harmed by a breach of its systems. Defendants further knew due to the nature of its business practices as a fully integrated health care delivery systems with dozens of hospitals, hundreds of doctors, and millions of patients, that a data breach could potentially result in the release of deeply personal, sensitive, and costly information about its patients.

47. Because PII is so sensitive and cyberattacks have become a rising threat, the FTC has issued numerous guides for businesses holding sensitive PII and emphasized the importance of adequate data security practices. The FTC also stresses that appropriately safeguarding PII held by businesses should be factored into all business-related decision making.

48. An FTC Publication titled "Protecting Personal Information: A Guide for Business" lays out fundamental data security principles and standard practices that businesses should implement to protect PII.[13] The guidelines highlight that businesses should (a) protect the personal customer information they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network's vulnerabilities; and (e) implement policies to correct security problems.

49. The FTC also recommends businesses use an intrusion detection system, monitor all incoming traffic to the networks for unusual activity, monitor for large amounts of data being transmitted from their systems, and have a response plan prepared in the event of a breach.

---

[13] https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business. (last accessed March 21, 2024)

50. The FTC also recommends that businesses limit access to sensitive PII, require complex passwords to be used on the networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.

51. Businesses that do not comply with the basic protection of sensitive PII are facing enforcement actions brought by the FTC. Failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data is an unfair act or practice prohibited pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45.

52. Many states' unfair and deceptive trade practices statutes are similar to the FTC Act, and many states adopt the FTC's interpretations of what constitutes an unfair or deceptive trade practice.

53. Defendants knew or should have known of its obligation to implement appropriate measures to protect its customers' PII but failed to comply with the FTC's basic guidelines and other industry best practices, including the minimum standards set by the National Institute of Standards and Technology Cybersecurity Framework Version 1.1.[14]

54. Defendants' failure to employ reasonable measures to adequately safeguard against unauthorized access to PII constitutes an unfair act or practice as prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45, as well as by state statutory analogs.

55. Defendants failed to use reasonable care in maintaining the privacy and security of Plaintiffs' and Class Members' PII and PHI. If Defendants had implemented adequate security measures, cybercriminals could never have accessed the PII of Plaintiffs and Class Members, and the Data Breach would have either been prevented in its entirety or have been much smaller in scope. For example, if Defendants had implemented adequate monitoring systems, they could have noticed and halted the approximately 6 terabytes of sensitive information purportedly downloaded by the hacker organization. Under normal circumstances no individual should be

[14] https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf. (last accessed March 21, 2024)

able to download even a tiny fraction of that information from the customer database and adequate monitoring should have flagged and stopped the exfiltrated data much earlier.

56. Moreover, a huge number of systems were compromised by the data breach. The number of compromised systems and the length of time it has taken to bring them back online suggests a fundamental security failure, including a failure to compartmentalize and secure access in the event of a breach. No one individual should ever be able to access all these systems. The extraordinary length of time the systems have been down suggests core systems including the source code (as some reports by the purported hackers say) may have been compromised. A reasonable cyber security system would not be able to be so fundamentally deficient. Finally, once Defendants became aware of the breach, they could have acted far faster and more aggressively in responding to the breach and in assisting victims in redressing harms, including sending notifications to those impacted of exactly what data was taken.

57. Personally Identifiable Information is of high value to criminals. Sensitive information can often be sold on the dark web, with personal information being sold at a price ranging from $40 to $200 and bank details with a price from $50 to $200.[15] The Data Breach exposed PII that is both valuable and highly coveted on underground markets because it can be used to commit identity theft and financial fraud. Identity thieves use such PII to, among other things, gain access to bank accounts, social media accounts, and credit cards. Identity thieves can also use this PII to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government identification cards, or create "synthetic identities." Additionally, identity thieves often wait significant amounts of time—months or even years—to use the PII obtained in data breaches because victims often become less vigilant in monitoring their accounts as time

[15] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed March 21, 2024).

passes, therefore making the PII easier to use without detection. Yet as of March 25, 2024, Defendants have failed even to offer free identity protection services for their customers. Given the extraordinary scale of the breach and the potential for consequences lingering for years. These identity thieves will also re-use stolen PII and PHI, resulting in victims of one data breach suffering the effects of several cybercrimes from one instance of unauthorized access to their PII and PHI.

58. Victims of data breaches are much more likely to become victims of identity fraud than those who have not. Data Breach victims who do experience identity theft often spend hundreds of hours fixing the damage caused by identity thieves.[16] Plaintiffs and members of the class generally have spent hours on end and considerable time and stress in attempting to mitigate the present and future harms caused by the breach. The U.S. Department of Justice's Bureau of Justice Statistics has reported that, even if data thieves have not caused financial harm, data breach victims "reported spending an average of about 7 hours clearing up the issues."[17]

59. The information compromised in the Data Breach—including detailed medical information—is much more valuable than the loss of credit card information in a retailer data breach. There, victims can simply close their credit and debit card accounts and potentially even rely on automatic fraud protection offered by their banks. Here, however, the information compromised is much more difficult, if not impossible, for consumers to re-secure after being stolen because it goes to the core of their identity. An individual's medical history and assessments are permanent and are impossible to escape. The loss of all this medical data puts Defendants customers and patients at additional risk for potential medical fraud and medical identity theft.

---

16 https://www.marylandattorneygeneral.gov/ID%20Theft%20Documents/Identitytheft.pdf. (last accessed March 21, 2024)

17 https://bjs.ojp.gov/content/pub/pdf/vit14.pdf. (last accessed March 21, 2024)

60. Data breaches involving medical records are not only incredibly costly, they can "also [be] more difficult to detect, taking almost twice as long as normal identity theft."[18] The FTC warns that a thief may use private medical information to, among other things, "see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care"[19] and that this may have far reaching consequences for a victim's ability to access medical care and use insurance benefits.

61. Security standards for businesses storing PII and PHI commonly include, but are not limited to:

a. Maintaining a secure firewall

b. Monitoring for suspicious or unusual traffic on the website

c. Looking for trends in user activity including for unknown or suspicious users

d. Looking at server requests for PII

e. Looking for server requests from VPNs and Tor exit notes

f. Requiring Multi-factor authentication before permitting new IP addresses to access user accounts and PII

g. Structuring a system including design and control to limit user access as necessary including a user's access to the account data and PII of other users.

62. Moreover, as Defendants themselves state in their privacy policy, not only do they aggregate PII and PHI from their patients, but they collect significant other information about the patients including profile pictures, social media accounts, information purchased from data brokers, marketing preferences/purchasing information, and government records. All this information will be extremely helpful to any malevolent entities that attempt to influence or

[18] *See What to Know About Medical Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited Nov. 22, 2023).
[19] *Id*

impersonate one of Defendants' patients. Defendants had an obligation to provide superior security in light of the sensitivity of the information they administered. Defendants failed.

63. Additionally, on its website privacy policy, Defendant Change healthcare claims that it "implement[s] and maintain[s] organizational, technical, and administrative security measures designed to safeguard the data we process against unauthorized access, destruction, loss, alteration, or misuse." It also claims that "Your Personal Information is only accessible to personnel who need to access it to perform their duties."[20]

64. However, by Defendants' own admission in February 2024 unauthorized agents who certainly did not "need to access it to perform their duties" accessed the personal information on millions of customers. Indeed, no single individual should ever "need to access" what appears to be the entire production server, including the private medical information on millions of patients. No single security failure should ever result in the disclosure of such information. Yet still the data was breached.

V. Plaintiffs' and Class Experiences

65. To use Defendants' Service, Plaintiffs provided sensitive PII and PHI including their full name, address, date of birth, social security number, medical records, insurance information, billing, banking, and credit card information, family medical history, and more. Although Defendants have not clarified specifically what information was compromised, on information and belief, released data on class members includes, but is not limited to: patient name and contact information including mail address, email address, and phone number; state and/or federal identification; social security number; health insurance information including healthcare cards; date of birth; medical information including information related to medical history, diagnosis, and treatment; information about treating physicians and medical professionals; billing and claims information including payment details, medication and prescription history; mental health information, contact information for family members

[20] https://www.changehealthcare.com/privacy-notice (Last Accessed March 21, 2024)

including full names, personal relationship, and phone number; Medicare/Medicaid information; workers comp or employment related information; and more.

66. Plaintiffs have taken reasonable steps to maintain the confidentiality of their PII and PHI. They relied upon Defendants' representations, experience, and sophistication to keep his information secure and confidential.

67. As a result of the data breach, Plaintiffs were forced to take measures to mitigate the harm, including spending time monitoring credit and financial accounts, researching the Data Breach, and researching and taking steps to prevent and mitigate the likelihood of identity theft.

68. As a result of the Data Breach, Plaintiffs suffered actual injuries including: (a) paying money to Defendants for services, which Plaintiffs would not have done had Defendants disclosed that they lacked data security practices adequate to safeguard Plaintiffs' PII and PHI from theft; (b) damages to and diminution in the value of Plaintiffs' PII—property that Plaintiffs entrusted to Defendants as a condition of receiving their services; (c) loss and invasion of Plaintiffs' privacy; (d) injuries arising from the increased risk of fraud and identity theft, including the cost of taking reasonable identity theft protection measures, which will continue for years, and (e) actual injury in fact for Plaintiff Nicholls due to being unable to continue prescribed medical treatment due to Defendants' compromised systems and being required to pay high out of pocket fees.

CLASS ACTION ALLEGATIONS

69. Plaintiffs bring this action as a class action pursuant to Rules 23(a) and 23(b)(1)-(3) of the Federal Rules of Civil Procedure, on behalf of themselves and a Nationwide Class defined as follows:

> **All persons in the United States whose PII/PHI were compromised by the Data Breach announced by Change Healthcare in February 2024.**

70. Excluded from the Nationwide Class are governmental entities, Defendants, any entity in which Defendants have a controlling interest, and Defendants' officers, directors, affiliates, legal representatives, employees, coconspirators, successors, subsidiaries, and assigns.

Also excluded from the Nationwide Class are any judges, justices, or judicial officers presiding over this matter and the members of their immediate families and judicial staff.

71. This action is brought and may be properly maintained as a class action pursuant to Rule 23. This action satisfies the requirements of Rule 23, including numerosity, commonality, typicality, adequacy, predominance, and superiority.

72. **Numerosity.** The Nationwide Class is so numerous that the individual joinder of all members is impracticable. While the exact number of Nationwide Class Members is currently unknown and can only be ascertained through appropriate discovery, Plaintiffs, on information and belief, allege that the Nationwide Class includes at least millions, perhaps tens of millions, of members based on widespread reporting and representations by Defendants.

73. **Commonality.** Common legal and factual questions exist that predominate over any questions affecting only individual Class Members. These common questions, which do not vary among Class Members and which may be determined without reference to any Class Member's individual circumstances, include, but are not limited to:

a. Whether Defendants knew or should have known that their systems were vulnerable to unauthorized access;

b. Whether Defendants failed to take adequate and reasonable measures to ensure their data systems were protected;

c. Whether Defendants failed to take available steps to prevent and stop the breach from happening or mitigating the risk of a long-term breach;

d. Whether Defendants unreasonably delayed in notifying patients of the harm they suffered once the suspicious activity was detected.

e. Whether Defendants unreasonably delayed in taking weeks to bring most of their systems back online, which cost patients and healthcare providers millions of dollars every day.[21]

[21] Some sources indicate losses may be at or above 100 million dollars per day.

f. Whether Defendants owed a legal duty to Plaintiffs and Class Members to protect their PII and PHI;

g. Whether Defendants breached any duty to protect the personal information of Plaintiffs and Class Members by failing to exercise due care in protecting their PII and PHI;

h. Whether Plaintiffs and Class Members are entitled to actual, statutory, or other forms of damages and other monetary relief; and,

i. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief or restitution.

74. **Typicality.** Plaintiffs' claims are typical of other Class Members' claims because Plaintiffs and Class Members were subjected to the same allegedly unlawful conduct and damaged in the same way.

75. **Adequacy of Representation.** Plaintiffs are adequate class representatives because they are Nationwide Class Members, and their interests do not conflict with the Class interests. Plaintiffs retained counsel who are competent and experienced in class action and data breach litigation. Plaintiffs and their counsel intend to prosecute this action vigorously for the Class' benefit and will fairly and adequately protect their interests.

76. **Predominance and Superiority.** The Nationwide Class can be properly maintained because the above common questions of law and fact predominate over any questions affecting individual Class Members. A class action is also superior to other available methods for the fair and efficient adjudication of this litigation because individual litigation of each Class member's claim is impracticable. Even if each Class member could afford individual litigation, the court system could not. It would be unduly burdensome if thousands of individual cases proceed. Individual litigation also presents the potential for inconsistent or contradictory judgments, the prospect of a race to the courthouse, and the risk of an inequitable allocation of recovery among those with equally meritorious claims. Individual litigation would increase the expense and delay to all parties and the courts because it requires individual resolution of common

legal and factual questions. By contrast, the class-action device presents far fewer management difficulties and provides the benefit of a single adjudication, economies of scale, and comprehensive supervision by a single court.

77. **Declaratory and Injunctive Relief.** The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members that would establish incompatible standards of conduct for Defendants. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other Class Members and impair their interests. Defendants have acted and/or refused to act on grounds generally applicable to the Class, making final injunctive relief or corresponding declaratory relief appropriate.

CLAIMS FOR RELIEF

Count 1
Negligence
On behalf of Plaintiffs and the Nationwide Class

78. Plaintiffs incorporate by reference and reallege each allegation above as though fully set forth herein.

79. Plaintiffs were required to provide PII and PHI as a precondition for using the Defendants' healthcare services.

80. Plaintiffs and Class Members entrusted their PII and PHI to Defendants with the understanding that Defendants would safeguard their PII and PHI.

81. In its written privacy policies, Defendants committed to taking reasonable steps to protecting patient PHI and PII. Defendants also acknowledged their obligation to abide by privacy regulations including HIPAA and committed to limit the degree to which this sensitive information was shared with other parties.

82. Defendants intentionally aggregated this information and combined this information with other information found on the web for their personal financial benefit, including the marketing of Defendants services.

83. Defendants claimed that "Your Personal Information is only accessible to personnel who need to access it to perform their duties."[22]

84. However, it appears millions of patients (including Plaintiffs) had their sensitive data accessed by hackers who had no "need" to access it.

85. Defendants did not take reasonable and appropriate safeguards to protect Plaintiffs and Class Members' PII and PHI.

86. Defendants had full knowledge of the sensitivity of the PII and PHI that it stored and the types of harm that Plaintiffs and Class Members could and would suffer if that PII and PHI were wrongfully disclosed.

87. Defendants violated their duty to implement and maintain reasonable security procedures and practices. That duty includes, among other things, designing, maintaining, and testing Defendants' information security controls sufficiently rigorously to ensure that PII and PHI in its possession was adequately secured by, for example, encrypting sensitive personal information, installing effective intrusion detection systems and monitoring mechanisms, using access controls to limit access to sensitive data, regularly testing for security weaknesses and failures, failing to notify patients of the specific breached data in a timely manner, and failing to remedy the continuing harm by unreasonably delaying notifying specific victims who were harmed.

88. Defendants' duty of care arose from, among other things,

a. Defendants' exclusive ability (and Class Members' inability) to ensure that its systems were sufficient to protect against the foreseeable risk that a data breach could occur;

b. Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, failing to adopt reasonable data security measures; and

[22] https://www.changehealthcare.com/privacy-notice (Last Accessed March 21, 2024)

c. Defendants' common law duties to adopt reasonable data security measures to protect customer PII and PHI and to act as a reasonable and prudent person under the same or similar circumstances would act.

89. Defendants' violation of the FTC Act constitutes negligence per se for purposes of establishing the duty and breach elements of Plaintiffs' negligence claim. Those statutes were designed to protect a group to which Plaintiffs belong and to prevent the types of harm that resulted from the Data Breach.

90. Defendants form a massive healthcare conglomerate with revenues in the hundreds of billions of dollars per year. Defendants had the financial and personnel resources necessary to prevent the Data Breach. Defendants nevertheless failed to adopt reasonable data security measures, in breach of the duties they owed to Plaintiffs and Class Members.

91. Plaintiffs and Class Members were the foreseeable victims of Defendants' inadequate data security. Defendants knew that a breach of their systems could and would cause harm to Plaintiffs and Class Members.

92. Indeed, some reports indicate dissenting voices warned Defendants about the danger of aggregating so much information in a single space as early as 2021 when UnitedHealth received pushback on its intended (and later completed) purchase of Change Healthcare. Defendants knew or should have known they were an extremely tempting target for attackers.

93. Defendants' conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Defendants' conduct included their failure to adequately mitigate harm through negligently failing to inform patients and victims of the breach of the specific information breached for (as of time of writing) more than a month after the purported first discovery of the breach.

94. Defendants knew or should have known of the inherent risks in collecting and storing massive amounts of PII and PHI, the importance of providing adequate data security for that PII and PHI, and the frequent cyberattacks within the medical industry.

95. Defendants, through their actions and inactions, breached their duty owed to Plaintiffs and Class Members by failing to exercise reasonable care in safeguarding their PII and PHI while it was in their possession and control. Defendants breached their duty by, among other things, their failure to adopt reasonable data security practices and their failure to adopt reasonable security and notification practices, including monitoring internal systems and sending notifications to affected victims. Defendants failed to timely notice Plaintiffs and Class Members of suspicious activities and failed to implement sufficiently stringent security measures.

96. Defendants inadequately safeguarded consumers' PII and PHI in breach of standard industry rules, regulations, and best practices at the time of the Data Breach.

97. But for Defendants' breach of their duty to adequately protect Class Members' PII and PHI, Class Members' PII and PHI would not have been stolen.

98. There is a temporal and close causal connection between Defendants' failure to implement adequate data security measures and notification practices, the Data Breach, and the harms suffered by Plaintiffs and Class Members.

99. As a result of Defendants' negligence, Plaintiffs and Class Members suffered and will continue to suffer the damages alleged herein.

100. Plaintiffs and Class Members are entitled to all forms of monetary compensation set forth herein, including monetary payments to provide adequate identity protection services. Plaintiffs and Class Members are also entitled to the injunctive relief sought herein.

Count 2
Breach of Implied Contract
On behalf of Plaintiffs and the Nationwide Class

101. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth above and incorporate them by reference as though set forth in full.

102. Plaintiffs and Class Members entered into an implied contract with Defendants when they entrusted Defendants with their PII and PHI.

103. As part of these transactions, Defendants agreed to safeguard and protect the PII of Plaintiffs and Class Members and to timely and accurately notify them if their PII or PHI was breached or compromised.

104. Plaintiffs and Class Members entered into the implied contracts with the reasonable expectation that Defendants' data security practices and policies were reasonable and consistent with the legal requirements and industry standards. Plaintiffs and Class Members believed that Defendants would use part of the monies paid to Defendants under the implied contracts or the monies obtained from the benefits derived from the PII and PHI they provided to fund proper and reasonable data security practices.

105. Plaintiffs and Class Members would not have provided and entrusted their PII and PHI to Defendants or would have paid less for Defendants' products or services in the absence of the implied contract or implied terms between them and Defendants. The safeguarding of the PII and PHI of Plaintiffs and Class Members was critical to realize the intent of the parties.

106. Plaintiffs and Class members fully performed their obligations under the implied contracts with Defendants.

107. Defendants breached their implied contracts with Plaintiffs and Class Members to protect their PII and PHI when they (1) failed to take reasonable steps to use safe and secure systems to protect that information; (2) disclosed that information to unauthorized third parties and; (3) failed to notify Plaintiffs and Class Members of the specific data breached a reasonably timely manner.

108. As a direct and proximate result of Defendants' breach of implied contract, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, medical identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market;

mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of their PII and PHI; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the Defendants' Data Breach; lost benefit of their bargains and overcharges for services or products; loss of access to medical services and treatment; overpayment for medical goods and treatments which should have been covered by insurance had Defendants' systems not failed, nominal and general damages; and other economic and non-economic harm.

109. As a direct and proximate result of the breach, Plaintiffs are entitled to relief as set forth herein.

Count 3
Unjust Enrichment
On behalf of Plaintiffs and the Nationwide Class

110. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth above and incorporate them by reference as though set forth in full.

111. Plaintiffs and Class Members entered into an implied contract with Defendants when they obtained products or services from Defendants, joined a healthcare program, or otherwise provided PII or PHI to Defendants.

112. As part of these transactions, Defendants agreed to safeguard and protect the PII and PHI of Plaintiffs and Class Members and to timely and accurately notify them if their PII or PHI was breached or compromised.

113. Plaintiffs and Class Members entered into the implied contracts with the reasonable expectation that Defendants' data security practices and policies were reasonable and consistent with legal requirements and industry standards. Plaintiffs and Class Members believed that Defendants would use part of the monies paid to them under the implied contracts or the

monies obtained from the benefits derived from the PII and PHI Plaintiffs and Class Member provided to fund proper and reasonable data security practices.

114. Plaintiffs and Class Members would not have provided and entrusted their PII and PHI to Defendants or would have paid less for Defendants' products or services in the absence of the implied contract or implied terms between them and Defendants. The safeguarding of the PII and PHI of Plaintiffs and Class Members was critical to realize the intent of the parties.

115. Plaintiffs and Class members fully performed their obligations under the implied contracts with Defendants.

116. Defendants breached their implied contracts with Plaintiffs and Class Members to protect their PII and PHI when they (1) failed to take reasonable steps to use safe and secure systems to protect that information; (2) disclosed that information to unauthorized third parties and; (3) failed to notify Plaintiffs and Class Members in a timely and reasonable fashion about the specific information breached.

117. As a direct and proximate result of Defendants' breach of implied contract, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, medical identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of their PII and PHI; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the Defendants' Data Breach; lost benefit of their bargains and overcharges for services or products; loss of access

to medical services and treatment; overpayment for medical goods and treatments which should have been covered by insurance had Defendants' systems not failed, nominal and general damages; and other economic and non-economic harm.

118. Defendants' annual revenue is in the hundreds of billions of dollars.

119. Customers who purchase Defendants' services do so with the reasonable belief that Defendants will appropriately protect the PHI and PPI they are entrusted with.

120. Had these customers known about Defendants' entirely insufficient data security policies they would not have used Defendants services or would have paid far less.

121. Defendants were unjustly enriched as a result.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class set forth herein, respectfully request the following relief:

A. That the Court certify this action as a class action and appoint Plaintiffs and their counsel to represent the Class;

B. That the Court grant permanent injunctive relief to prohibit Defendants from continuing to engage in the unlawful acts, omissions, and practices described herein and directing Defendants to adequately safeguard the PII and PHI of Plaintiffs and the Class by implementing improved security controls;

C. That the Court award compensatory, consequential, and general damages, including nominal damages as appropriate, as allowed by law in an amount to be determined at trial;

D. That the Court award statutory or punitive damages as allowed by law in an amount to be determined at trial;

E. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of Defendants' unlawful acts, omissions, and practices;

F. That the Court award to Plaintiffs and Class Members the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses; and

G. That the Court award pre- and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demands a jury trial on all claims so triable.

Dated: March 27, 2024

/s/ J. Gerard Stranch, IV
J. Gerard Stranch, IV, BPR 23045
Michael Iadevaia, BPR 041622
Emily Schiller, BPR 039387
STRANCH, JENNINGS & GARVEY PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
Telephone: (615) 254-8801
gstranch@stranchlaw.com
miadevaia@stranchlaw.com
eschiller@stranchlaw.com

SCHUBERT JONCKHEER & KOLBE LLP
ROBERT C. SCHUBERT* (rschubert@sjk.law)
AMBER L. SCHUBERT* aschubert@sjk.law)
2001 Union St, Ste 200
San Francisco, CA 94123
Tel: (415) 788-4220
Fax: (415) 788-0161

Attorneys for Plaintiffs and the Proposed Classes

**Pro hac vice* forthcoming